

TRANSMITTAL SLIP / NOTE D'ENVOI

To / À DIRECTOR		Classification TOP SECRET	
From / De ADP		File / Dossier 2016 06 27	
Drafting officer / Rédacteur		Date 2016 06 27	
Subject / Sujet Briefing Note to the Minister: Update on <i>en banc</i> hearings and the Service's retention and destruction of warranted collection			
Action / Donnez suite		Deadline / Délai	
<input checked="" type="checkbox"/> Signature <input type="checkbox"/> Comments / Commentaires <input checked="" type="checkbox"/> Approval / Approbation <input type="checkbox"/> Information		2016 06 27 COB	
Priority / Priorité			
<input checked="" type="checkbox"/> Routine <input type="checkbox"/> Urgent <input type="checkbox"/> Immediate / Immédiate			
Record of Consultation/Approval Rapport de consultation/d'approbation		Comments / Commentaires	
Consulted Consulté Concur D'accord Yes Oui No Non		As per your request, please find enclosed a memorandum for your signature to the Minister of Public Safety Canada (PSC) providing an update on the Canadian Security Intelligence Service's (CSIS) involvement in the <i>en banc</i> hearings. In addition, the memorandum also provides an update on your appearance in Federal Court in June 10, 2016. As well, it notes that the report outlining the Service's	
DLS A/Chief Chief, DDO DG, PFR ADL Jun 27 2016 see email attached		CSIS / SCRS JUN 27 2016 24382 DIR CSIS / SCRS JUN 27 2016 24382 ADP / DAP	



Director - Directeur

Service canadien du
renseignement de sécurité

CCM #24382

TOP SECRET

For Information

JUN 29 2016

MEMORANDUM TO THE MINISTER

**UPDATE ON *EN BANC* HEARINGS AND THE SERVICE'S RETENTION AND
DESTRUCTION OF WARRANTED COLLECTION**

ISSUE:

Further to my memorandum of April 11, to provide an update regarding the Canadian Security Intelligence Service's (CSIS) involvement in *en banc* hearings, as well as related engagements with the Federal Court.

BACKGROUND:

In early 2016, CSIS sought to renew and obtain new warrants for targeted individuals, while also proposing amendments to warrant conditions. The application was heard *en banc*, or as a panel. At that hearing, the Court indicated that it wished to more thoroughly examine the impact that section 12 warrants may have on third parties. The hearing resumed on March 31 and April 1 and the Court requested written submissions to determine whether the wording of warrants, as proposed, strikes an appropriate balance between CSIS operational needs and third party privacy rights. The Court also requested submissions pertaining to the legal basis pursuant to which CSIS has retained associated data since 2006. In support of these requirements, CSIS filed two affidavits on April 21 and submissions on June 22.

DISCUSSION:

The Court has continued to issue warrants

A decision is not expected until fall 2016, which

As we do not expect a decision from the Court in these matters before the last part of October,

In addition, my previous memorandum noted that the Attorney General of Canada provided information to the Court regarding the Security Intelligence Review Committee's (SIRC)

findings regarding the Service's transparency with the Court on issues related to associated data filed on June 8.

On June 10, I appeared before the Federal Court with the Deputy Minister of Justice to address issues identified by the Court in relation to transparency and duty of candor. We presented a series of measures proposed to address the issues identified by the Court, including the adoption of a joint policy on the duty of candour in *ex parte* proceedings and the review of collection, retention, and destruction practices related to the execution of warrants.

In addition, I undertook to advise the Court promptly of matters relevant to applications for warrants as they may become identified pursuant to internal audits or SIRC reviews. I also reiterated CSIS' commitment to resolving the matters identified by the Court, and to implement corrective measures as they are identified. Throughout, I emphasized full mindfulness of the Service's duties in terms of candour and the rule of law.

On a related matter, further to my May 26 memorandum to you regarding the

The

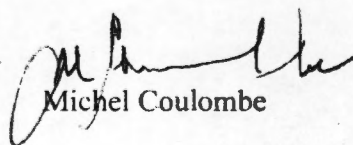
Court acknowledged having received the report.

NEXT STEPS:

The Service has initiated a review of the business and technical systems used for the collection, retention or destruction of information acquired pursuant to a warrant. The objective is to identify and address any gaps to guarantee the highest level of assurance of compliance with warrant conditions, including a governance mechanism with clear points of accountability. An initial report is scheduled to be provided to me in late September, 2016.

I wish to reiterate that the Service has and will continue to take its duty of candour very seriously and will continue to work in a forthright manner with the Court. I will keep you apprised of any new developments.

As always, please do not hesitate to contact me should you require further information.


Michel Coulombe

cc: Deputy Minister, Public Safety

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

TRANSMITTAL SLIP / NOTE D'ENVOI

To / À DIRECTOR cc: DDO		Classification TOP SECRET	
From / De ADP		File / Dossier	
Drafting officer / Rédacteur		Date 2016 10 13	
Subject / Sujet Memorandum to the Minister: En Banc: Federal Court Decision on Warrant Conditions and Retention of Data Associated with Third Party Communications			
Action / Donnez suite		Deadline / Délai	
<input checked="" type="checkbox"/> Signature <input type="checkbox"/> Comments / Commentaires <input checked="" type="checkbox"/> Approval / Approbation <input type="checkbox"/> Information		<input type="checkbox"/> Routine <input type="checkbox"/> Urgent <input checked="" type="checkbox"/> Immediate / Immédiate 2016 10 13 (16:00)	
Record of Consultation/Approval Rapport de consultation/d'approbation		Comments / Commentaires	
Consulted Consulté Priority / Priorité Yes Oui No Non		Concur D'accord Yes Oui No Non	
DDO DLS Chief, DG, PFR ADL ADE ADP		Please find enclosed for your signature a Memorandum to the Minister in relation to the Federal Court decision on warrant conditions and retention of data associated with third party communications. This is as a result of the four days of <i>en banc</i> hearings that occurred in February, March and April 2016. <i>note</i> <i>very good</i> <i>for board</i>	



CCM#25140

TOP SECRET
For Information

OCT 14 2016

MEMORANDUM TO THE MINISTER

**EN BANC: FEDERAL COURT DECISION ON WARRANT CONDITIONS AND
RETENTION OF DATA ASSOCIATED WITH THIRD PARTY COMMUNICATIONS**

SUMMARY

- Further to my memoranda of April 11 and June 29, to inform that on October 4, 2016 the Federal Court issued its judgement and reasons in relation to the Canadian Security Intelligence Service's (CSIS) proposed amendments to section 12 warrant conditions, as well as its retention of data associated to third party communications.
- Though the Court accepted a number of the Service's proposed wording changes to warrant conditions, it found that CSIS breached its duty of candour by failing to fully and transparently inform the Court of its retention program, and that its retention of associated data linked to third party communications found to be unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs is illegal.

BACKGROUND:

In December 2015, CSIS sought to renew and obtain new warrants for targeted individuals, while also proposing amendments to certain warrant conditions. The application was heard *en banc*, or as a panel. Owing to a finding in the Security Intelligence Review Committee's (SIRC) annual report (2014-15) that the Service's transparency with the Federal Court regarding the collection, use, retention and destruction of associated data (referred to by SIRC as metadata) collected under warrants was insufficient, the Court requested that this matter also be addressed.

it is defined as data collected through warranted operations from which the content was assessed as unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs.

The *en banc* hearings on these matters were held over four days in February, March and April 2016. Five affidavits were filed and three affiants were examined, and both written and oral submissions were made addressing the establishment of the Operational Data Analysis Centre (ODAC), the retention of associated data, and operational reasoning behind the proposed wording changes to warrant conditions.

Following an exchange of letters between the Assistant Deputy Attorney General and the Chief Justice of the Federal Court, the Court called for another *en banc* hearing to address perceived issues arising from CSIS' candour towards the Court in relation to the retention program of associated data and other related concerns. Thus, on June 10, I appeared before the Federal Court along with the Deputy Minister of Justice.

DISCUSSION:

The Federal Court's decision, which was issued by the Honourable Justice Noël on October 4, deals with three particular issues. These include: whether the Service breached its duty of candour toward the Court when it established and ran the Operational Data Analysis Centre (ODAC) program; whether the Service is legally authorized to retain associated data linked to third party (i.e. non-target) communications unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs; and whether the Service's proposed amendments to warrant conditions were acceptable.

Though no evidence indicated this was deliberate, the Court found that CSIS breached its duty of candour by omitting to inform the Court, between 2006 and 2016, of the Service's new position on the retention of data, as well as ODAC's creation. I take seriously the concerns of the Court, and commit to, going forward, advise the Court of changes in policy or practice relevant to the exercise of our warrants without delay. That said, since its establishment, the Service has sought to provide the necessary policy and guidance for employees to ensure compliance with the law and Ministerial Direction. To that end, CSIS has, through its dealings with the Court, acted based on consistent advice from the Department of Justice. As the Court acknowledges, however, the *CSIS Act* of 1984 was not drafted to account for the enormous and unforeseen technological advances of the last decade.

The Court also found that the Service's retention of associated data linked to third party communications is illegal. The decision argues that the 'strictly necessary' qualifier in s.12 of the *CSIS Act* applies to both collection under s.12 and retention of collected information, including that which is obtained pursuant to a warrant issued under s.21. From this perspective, incidental collection of associated data linked to third parties not found to be related to any threats is not considered to meet the 'strictly necessary' qualifier.

Associated data linked to third parties not found to be related to any threats is susceptible to being collected as a consequence of a warranted operation on a target. Justice Noël concludes,

however, that as this is not within the scope of the warrant, nor is it the reason for the warrant to be granted, a determination must be done, within a short period, to assess the relevance of this data to the target or threats to the security of Canada.

Though the Service may continue to retain associated data linked to a target's communications, it will no longer be able to retain associated data linked to third party communications found to be unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs. This is a shift from current practice, as since 2006, CSIS has retained all associated data and inserted it into ODAC for future investigative purposes.

Given the decision, CSIS has halted internal use and analysis of all associated data.

Given the requirement to assess, within a short period, relevance to targets or threats to the security of Canada, the Service has been given three months to implement a two-step process of assessment. As outlined in the decision, upon successful decryption or decoding, the Service will have six months to assess information and communications that are obviously unrelated to a target or a threat. The Service will continue to have 12 months for other communications and information.

Of note, the Court was satisfied with a number of the Service's proposed amendments to s.12 warrant conditions. Amongst other things, it accepted the Service's proposal to:

As these proposals to amend warrant conditions initiated the *en banc* hearings, this aspect of the decision is positive.

NEXT STEPS:

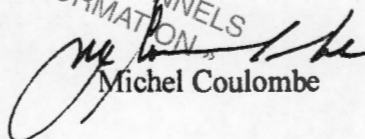
"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
"RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION"

Though not directly related, I have also exerted particular emphasis on employee responsibilities as it pertains to operational compliance. This, given that it is the foundation for maintaining the trust and confidence of CSIS' domestic and foreign partners, the Court and the Canadian public. Work is therefore underway to enhance the Service's compliance management framework for all of its operational activities, as well as increase resources dedicated to operational compliance.

A redacted version of the Federal Court's judgement and reasons could be made available to the public as early as October 18, though this will depend on the Court's review of the redactions due that day. This will likely garner attention and, given the Court's critical stance, there will likely be reputational impact on the Service at a moment when the public and stakeholders have been actively engaged by you. In addition to the heightened attention brought by the consultations, the Privacy Commissioner, who recently tabled his annual report addressing Bill C-51, amongst other things, will also be interested in this decision.

I wish to reiterate that the Service recognizes the importance of compliance with Ministerial Direction and the CSIS Act, as well as openness and transparency with the Court. Moreover, I wish to emphasize that CSIS will improve its practices involving the Court to ensure that duty of candour-related issues do not occur again.

As always, please do not hesitate to contact me should you require further information.


Michel Coulombe

cc.: National Security Advisor
Deputy Minister, Public Safety

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.



Director / Directeur

CCM # 23637

TOP SECRET
For Information

AVR 11 2016

MEMORANDUM TO THE MINISTER

FEDERAL COURT WARRANT EXAMINATION: EN BANC HEARING

SUMMARY

- On 25 and 26 February, the Canadian Security Intelligence Service (CSIS) appeared in an *en banc* hearing before the Federal Court in relation to proposed amendments to six section 12 warrant conditions and to the category of employees that may make determinations pursuant to the matter was continued on 31 March and 1 April.
- The Federal Court expressed appreciation with the information provided by the Service thus far. The Court requested legal submissions on issues that will require further evidence on the utility of associated data and the circumstances surrounding the Service's decisions on retention of associated data since 2006.

BACKGROUND:

In the course of an investigation, CSIS may obtain warrant powers against targets to authorize the use of specific investigative techniques. These powers allow CSIS to intercept communications destined to, received by, or originating from, devices or accounts that are owned by a target. They also allow CSIS to In certain circumstances, the Service may execute warrant powers in relation to

Execution of any of these warrant powers may result in the incidental collection of information from parties other than the target (i.e. third parties).

When the Service intercepts communications, it obtains the content of the communication, as well as its associated data (referred to by the Security Intelligence Review Committee (SIRC) as metadata). Associated data is information, in structured fields, linked with a communication. Examples include email addresses, telephone numbers, as well as duration, dates and

times of phone calls or Internet sessions. It does not include any information that could reveal the purpose of the communication, nor any part of its content.

Existing policies and procedures require that, subject to the exception for data related to solicitor-client communications, which is deleted immediately, information and communications intercepts collected under warrant, whether from a third party or not, found to be of no intelligence value be destroyed. This policy, however, does not apply to associated data.

DISCUSSION:

On 25-26 February 2016, CSIS sought to renew and obtain new warrants for targeted individuals, while also proposing amendments to warrant conditions. The application was heard *en banc*, or as a panel. While the Court was satisfied that the threat to the security of Canada posed by the activities being investigated had been established, it did not render a decision on the Service's proposed amendments to warrant conditions.

At that hearing, the Court indicated that it wished to more thoroughly examine the impact that section 12 warrants may have on third parties. It also requested that the Service provide further evidence regarding the collection, use, retention and destruction of associated data collected under warrants issued by the Court. This, owing to a finding in SIRC's annual report (2014-15) that the Service's transparency with the Federal Court in this regard was insufficient.

Further to the hearing and in response to the Court's request, CSIS filed two supplemental affidavits. The first described the process used to manage the way in which the Service conducts its warranted collection.

particular emphasis was placed on the manner in which CSIS may execute warrants related to

The second affidavit addressed the Service's collection, processing, use and retention of associated data, including several examples of the foregoing and an analysis of its investigative value. Through this affidavit, CSIS also proposed that associated data related to third party communications intercepts found to be of no intelligence value be retained for a period of

This is a shift from current practice, whereby no such limit exists. Both affidavits included several examples aimed at demonstrating that there is an operational need that justifies the retention of associated data and that measures are in place to limit the impact on third parties.

The hearing resumed on 31 March and 1 April. While the Court was appreciative of the Service's illustration that associated data is valuable, questions remain regarding the value of retaining associated data over time. As such, CSIS will be offering further evidence to address this issue.

The Court requested written submissions to determine whether the wording of warrants, as proposed, strikes an appropriate balance between CSIS operational needs and third party privacy rights. The Court also requested submissions pertaining to the legal basis pursuant to which CSIS has retained associated data since 2006, when this practice appears to have begun. In response,

the Service will file an affidavit including evidence of the circumstances surrounding the Service's decisions related to the retention of associated data since 2006.

It is anticipated that the Court will be satisfied with the proposed amendments to section 12 warrant conditions, with minimal amendments to the proposed wording. These allow the Service to

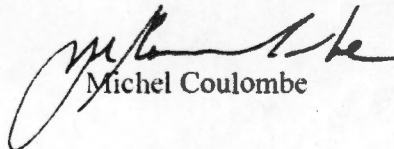
Other new conditions specifically govern
prevent the Service from retrieving information that was destroyed pursuant to a warrant condition; and, alter the designated employees in warrant conditions relating to the retention of information and communications.

NEXT STEPS:

On 7 April, the Service advised the Court that it will be filing two additional affidavits. The first will pertain to the utility of associated data and the second will pertain to the circumstances surrounding CSIS' decision to, in 2006, retain associated data. Provided that the Court is in agreement with this proposal, both affidavits will be filed by 21 April. CSIS will submit legal submissions shortly after, at a date to be set by the Court.

Of note, on 7 April, the Attorney General of Canada provided information to the Court related to SIRC's findings regarding the Service's transparency with the Court on issues related to associated data. This was provided in response to a 23 March request from the Honourable Chief Justice Crampton, who requested this information to assist the Court in understanding the basis upon which SIRC formulated its recommendation. It is possible that the information provided by the Attorney General will further inform the designated judges sitting in the *en banc* hearing.

I wish to reiterate that the Service takes its duty of candour very seriously and will continue to work in a forthright manner with the Court. I will keep you apprised of any new developments. As always, please do not hesitate to contact me should you require further information.


Michel Coulombe

National Security Advisor
cc.: Deputy Minister, Public Safety

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.